4104013001-00018-00
Date: 03/19/2004

Functional Description

for the

Generation-3
Personnel Safety System
(PSS)

of the

Advanced Photon Source

at

Argonne National Laboratory
9700 Cass Avenue
Argonne, Illinois 60439

WBS x.1.4.1.4.1.30.1

APPROVED BY

John Carwardine, Associate Division Director, Electrical Systems, ASD	Date
, Group Leader, SI, ASD	Date
Mohan Ramanathan, Chairman, Adhoc Gen 3 PSS committee	Date
James Lange Radiation Safety	Date

PREPARED BY

Roy Emerson, Date
SI, ASD

REVIEWED BY

Jon Hawkins, Date
SI, ASD

Nick Friedman, Date
SI, ASD

Martin Knott, Date
ESS, ASD

John Servino, Date
SI, ASD Consultant

(INDEX) **INDEX OF PAGE REVISIONS**

PAGE NO.	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
REV. NO.	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

PAGE NO.	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
REV. NO.	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

PAGE NO.	31	32	33	34	35	36	37	38	39						
REV. NO.	00	00	00	00	00	00	00	00	00						

PAGE NO.															
REV. NO.															

PAGE NO.															
REV. NO.															

PAGE NO.															
REV. NO.															

REVISION AUTHORIZATION

REVISION NUMBER	00	01	02	03	04	05	06	07	08
DCN NUMBER									
DATE									
APPROVED BY									

Table of Contents

1. Purpose

Develop a new PSS interlock system to be used as the standard implementation for new beamline builds.

2. Scope of Document

This document is limited to the functional description of the Beamline PSS at the Advanced Photon Source.

3. Responsibilities and Assumptions

3.1 Field devices

All field devices previously reviewed and approved for use in Version-1 PSS such as strobe lights, relays, limit switches for doors and shutters, speakers, etc. will be used in Generation-3 PSS systems. The safety evaluation process is significantly enhanced by using these approved devices and the considerable operational experience that has been gained with them.

3.2 Pneumatic controls

The construction, installation and maintenance of pneumatic controls for front-end shutters, beamline shutters, station doors and the equipment they control is the responsibility of another group. The Safety Interlocks Groups responsibility will include wiring to a common interface connection point for the devices in a control panel supplied by the other group. The Safety Interlocks Groups will also participate with the calibration and validation of the devices to insure proper operation with the PSS.

3.3 De-Ionized Water controls

The construction, installation and maintenance of the De-Ionized water system, including the sensors for water flow and water pressure is the responsibility of another group. The Safety Interlocks Groups responsibility will include wiring to a common interface connection point for the sensors in a control panel supplied by the other group. The Safety Interlocks Groups will also participate with the validation of the devices to insure proper operation with the PSS.

4. Operational and Safety Considerations

- Meet the safety and operational needs of the APS beamlines in a cost-effective manner
- Meet the operational and reliability needs of APS machine and beamline operations
- All logic used in this system whether programmed or hardwired will be positive true.
- The design is to be inherently fail-safe in that loss of a signal or voltage or component failure will result in a safe state.
- The design will comply with all of the issues mandated by the documents in the section **Applicable Documents** and with good and standard practices at the time of design.
- The design will be reviewed periodically to insure it conforms to current safety practices.

5. Applicable Documents

5.1 Government Documents

The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement.

DOE ORDER 420.2, 11-5-98

Accelerator Safety Implementation Guide for DOE O 420.2, Draft, May 1999

DOE ORDER 5480.25, 11-3-92

DOE GUIDANCE 5480.25, September 1, 1993

Copies of specifications, standards, drawings and publications required by suppliers in connection with specified procurement functions should be obtained from the contracting agency or as directed by the contracting office.

5.2 Non-Government Documents

The following documents are part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement.

APS Safety Assessment Document (SAD), Rev 1, May 1999, Argonne National Laboratory, Argonne, IL.

Argonne National Laboratory Environment, Safety & Health Manual, May 27, 1999

Compliance with the following required by SAD

SLAC Report 327, April 1988, Stanford Linear Accelerator Center, Menlo Park, CA.

NCRP Report No. 88, Issued 30 December 1986, National Council on Radiation Protection.

NBS Handbook 107, "Radiological Safety in the Design and Operation of Particle Accelerators," ANSI N43.1 (NBS 1979).

Technical society and technical association specifications and standards are available for reference through their respective associations.

6. APS Personnel Safety System (PSS)

6.1 Introduction

The APS has the potential of operating with up to 70 beamlines. Each beamline includes multiple shielded enclosures containing optics and experimental equipment. Personnel access into these enclosures will be controlled during beamline operation. The APS Personnel Safety System (PSS) is the engineered safety system for each beamline for controlling access into the enclosures, ensuring that access is allowed only under safe conditions (i.e., beam is off in the enclosure), and to disable storage ring operation if improper access is gained or a PSS system fault is detected that could potentially endanger personnel.

The PSS for each beamline interfaces directly with the Accelerator Systems Access Control and Interlock System (ACIS) for disabling storage-ring operation. Each PSS is totally isolated from the PSS of any other beamline to prevent a fault from one beamline affecting the PSS system of other beamlines.

Each beamline PSS is designed by APS Safety Interlocks Group staff to meet the requirements of the individual Collaborative Access Team (CAT) after review and concurrence by the Beamline Review Committee (BRC). The APS Safety Interlocks Group staff is also responsible for the installation, verification and regular testing, and any required maintenance of the system. Although beamline designs require some flexibility in possible modes of operation, types of devices to be interlocked, and other operational requirements, the basic configuration and control aspects will remain the same. Specialized control panels will be designed to incorporate any special features. The system documentation, test procedures, and training will include all basic as well as specialized equipment and operating modes.

The PSS is designed to comply with the following:

- DOE Order 5480.25, "Safety of Accelerator Systems" (DOE 1992b).
- "APS Preliminary Safety Analysis Report" (ANL 1990).
- SLAC 327, "Health Physics Manual of Good Practices for Accelerator Facilities" (SLAC 1988).
- NBS Handbook 107, "Radiological Safety in the Design and Operation of Particle Accelerators," ANSI N43.1 (NBS 1979).
- NCRP Report No. 88, "Radiation Alarms and Access Control Systems" (NCRP 1986)

Among the more important aspects of conformance, the PSS satisfies the following requirements:

- The system is designed to be fail safe, so common failures (e.g., shorts to ground or open wires) leave the system in a safe, beam-off state.
- The system is incorporates redundant isolated feedback to detect failed critical outputs.
- The design incorporates redundant protection, ensuring that no single component or subsystem failure leaves the system in an unsafe, beam-on condition.
- Provisions for testing are included, so that proper component and system functions may be completely verified.
- Access and egress controls are incorporated so that personnel are not exposed to x-ray radiation. These include emergency shut-off devices, status signs, search and secure procedures, and emergency exit mechanisms.
- A document control and review system is incorporated for keeping documentation complete, accurate, and current.
- A strict configuration control system protects the circuits and software against unauthorized and inadvertent modification. Critical devices are clearly labeled to note that tampering is strictly forbidden.
- User training for proper system operation is incorporated and users are made aware of the consequences of tampering or improper use of the PSS.

7. Beamline Personnel Safety System (PSS) Description

7.1 Overview

Each beamline PSS contains a Command and Control processor (Chain-C) and two independent redundant interlock chains, referred to in this document as Chain-A and Chain-B. The PSS Chain-A and Chain-B interlock chains provide the redundant Emergency Shut Down (ESD) function for the PSS and are referred to interchangeably in this document. The PSS incorporates the following equipment:

- Programmable Logic Controllers (PLCs) are installed in each chain to perform the system's protective decision logic.
- PLC input/output (I/O) modules which interface the PLCs with the switches, lights, locks, relays, and other devices used by the PSS.

- Centralized uninterruptible power supply (UPSs) to protect against short-term AC power loss.
- User Interface panels and status displays.
- Station door hardware (status switches, locking mechanisms).
- Station search-and-secure hardware (search buttons, visible and audible warning indicators, emergency shutdown buttons).
- Interfaces to beam shutdown safety devices, such as front-end or beamline safety shutters and photon shutters (position-indicating switches and position-controlling solenoids).
- Interfaces to the ACIS (for storage ring shutdown), the Front-End Equipment Protection System (FE-EPS), the Beamline Equipment Protection System (BL-EPS) (for monitoring and control), and the EPICS control system (for status display and diagnostics).
- Equipment racks, conduit, cable trays, and cables.

The concern of common mode failures in redundant protection systems is addressed by using different hardware and software platforms for the two chains. Using different programmers to develop the software for each chain further reduces the probability of a common mode failure.

A programming key is required to program the PLC or to operate the PLC in a non-normal mode and once this key is removed from the PLC CPU module, the PSS program cannot be modified by any external means.

Each interlock PLC crate has a unique hardwired address that encodes the beamline number (1 to 35) and type (ID or BM). This address is set at initial construction of the beamline and will never change during the life of the system. This associates a crate with a particular beamline. During software execution, one of its regular tasks is to verify, via the crate ID number, that it is operating in the intended crate (and therefore the proper beamline). The crate address insures that the software written for another beamline will only run on the beamline it was written for. The PLC crate also has a unique hardwired software version number from 0 to 255. This version number is incremented with each new build of the software. When incremented from 255 the new value will be 0. The software version number is used to prevent any version except the correct version from running. This version number must be changed at the beamline prior to validating the new software build.

Each interlock PLC has two watchdog timers. The first is a user programmed pulsed signal .5 seconds on and .5 seconds off. The opposite interlock PLC (Chain-A or Chain-B) will monitor this signal. If the signal is lost, the PLC detecting the loss, will generate a programmed fault identifying the cause and close the Front End Shutters. This fault will require correction of the problem and a manual reset of the system to re-enable operation. Second, an on-board hardware verification, which checks the integrity of the data and address busses, is executed every scan of the logic. A detected fault will cause the PLC to stop processing and all local and remote outputs

to be de-energized. These outputs control critical devices and the permits to the ACIS. This fault will abort the stored beam and insert all safety shutters.

The PLCs, UPS, and interface modules for the ACIS, FE-EPS, BL-EPS, and front-end components for both interlock chains are located in locked relay racks located on the top of the storage ring tunnel and are inaccessible to the users.

Equipment to which the user needs access, such as door controls and mode controls, are located in equipment cabinets located on or near the experiment stations. The equipment cabinets are locked to prevent uncontrolled access to wiring. These cabinets also contain the I/O modules for the PSS equipment at the station location. The front of the cabinets contain all of the user accessible controls for normal beamline operation.

APS experimental station control panels provide:

- A visual indication of the beamline station access status (Access Allowed or Access Denied)
- Beamline safety shutter controls
- Beamline door status indicators and controls
- The means to switch shutter control between stations on a beamline
- The mechanisms to administratively take stations off-line and bring them back on-line
- Status indicators for program detectable fault conditions and a means to reset them
- Optional mode shutter status indicators and the special controls required by them

7.2 Beamline

7.2.1 Field devices

The Field devices are all of the devices used as sensors providing input to the PSS or as controlled devices performing some action when activated by the PSS. For all PSS field devices such as (door switches, speakers, search boxes, etc) Generation-3 PSS will use the devices previously reviewed and approved for use in Version-1 and Version-2 systems.

7.2.2 Stations

7.2.2.1 Experimental Station Hardware

7.2.2.1.1 Doors

The experimental station doors may be operated manually or by powered means, such as with an air cylinder. However, the PSS hardware for the door is the same in all cases and consists of:

- A manual or electronic door lock to hold the door fixed in place.
- Door status switches, provided for each interlock chain, indicating that the door is closed.
- Pneumatic doors have a door control box as shown in Figure 1.

Figure 1

7.2.2.1.2 Emergency Egress

Emergency entrance and egress mechanisms are located on the inside and outside of the station door. The PSS door hardware does not interfere with the access/egress mechanism operation. A typical emergency egress panel is shown in Figure 2.

Figure 2

7.2.2.1.3 Emergency Stops (Crash Buttons)

One or more emergency shutdown switches ("crash buttons") will be provided to inhibit storage-ring operation when depressed if the station is beam active. The number of emergency shutdown switches is determined during the BRC design review process and is based on the design of the enclosure and the equipment it will contain to ensure easy accessibility from any location within the enclosure.

Typical emergency stop buttons are shown in Figure 3.

Figure 3

7.2.2.1.4 Search Boxes

The inside of the station contains one or more search buttons with visual and audible indicators of a search in progress. The number of search buttons is determined during the BRC design review process and is based on the design of the enclosure and the equipment it will contain. The search buttons must be depressed in the correct sequence, and the search must be completed and the door closed within a predetermined interval for the search to be considered successful by the PSS logic. The Search and Secure status is one of several interlocks necessary to open the shutters. The search buttons are shown in Figure 4.

Figure 4

Figure 4

7.2.2.1.5 Audible and Visual Warnings

The visual warning consists of one or two red strobe lights that are turned on at the start of the search. The strobe lights will remain on until the search has completed or has been aborted by one or more of the conditions listed under Aborting the Search. Typical strobe lights and speakers for these warnings are shown in Figure 5.

Figure 5

7.2.2.1.6 Mirrors

Due to the placement of user equipment, in some stations, mirrors may be required to be placed in hard to access areas. The mirrors, if used, will allow the person searching the station to determine if someone is in one of the hard to access but not impossible to reach areas.

7.2.2.2 Station User Controls

A station control panel is used to open and close safety shutters, gain safe access to the experimental station, and provide visible feedback regarding the states of the accelerator permits, other experimental stations, and the shutters. The control panel will also contain the necessary circuits for operation of the station and shutters. And finally it will provide test connectors for verification and validation. A typical user station control panel will look like Figure 6.

Figure 6

7.2.2.2.1 Station Status Display

The status display consists of a chain of simulated LED indicators that are laid out in a manner consistent with the beamline layout. The indicators are green if the related devices or systems permit the beam to be propagated down the beamline and are red

if configured to stop the beam. The beamline safety-shutter and station-enable controls are located on the panel next to the appropriate indicators.

7.2.2.2.2 APS Enable Key

The Station APS Enable key is used by the APS facility to administratively enable the station for beam or keep it off-line (shutters closed and disabled). This is the key used by the Floor Coordinator to shut down a beamline or section of a beamline due to safety, operational, or other concerns. Each station in a beamline will have an APS key. The APS key is used to toggle on or off the APS Enabled state for a station. The APS Enabled state is an interlock in the shutter open logic for the shutter that protects the station it is located at. If the station protective shutter is open when the APS Enabled state is toggled to off, the shutter will be closed.

7.2.2.2.3 User Key

The Station User key(s) allows a user to lock out the shutter control for an active on-line station and allows administrative control by the user of the operation of a beamline or section of the beamline.

7.2.2.2.4 Mode Shutters

The Beam Mode indicators show the type of beam that is in the station. The mode of the beamline is the hardware configuration identified by the type of radiation (e.g., white beam or monochromatic beam) that will be propagated as well as where the radiation can be propagated (e.g., down a particular branch line or through a bypass). The mode is determined by the positions of instruments, such as mirrors, monochromators, shielding, stops, etc.

7.2.2.3 Shutter Mode Controls

For each ID or bending-magnet beamline that has more than one interlocked mode of operation, a mode selection panel is provided. This panel captures the PSS Kirk keys for stops, shutters, etc., when they are released from matching locks located on the devices when beamline operating modes are changed. The PSS monitors not only the position of mode changing devices (stop or shutter position) but also the location of the Kirk keys. The device positions and keys must match a predetermined state for the particular mode to be enabled. When the interlocks have been satisfied for a mode, this will be indicated on the Mode Selection Panel as well as on the Station Control Panels. The complexity and variability of beamline operation will determine the number and location for the mode control panels. The panel layout for a typical mode selection panel is shown in Figure 7.

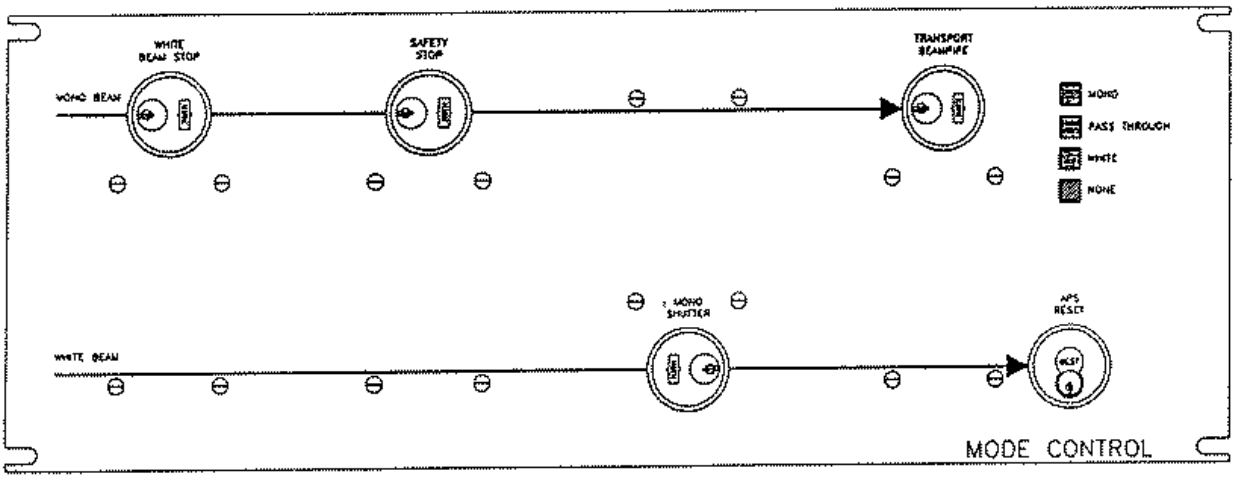

Figure 7.

Depending on the design and operating requirements of the beamline, certain mode changes may require APS intervention/concurrence through the use of a facility-controlled key. This key is designated the Mode Select key and is keyed the same as the floor coordinators APS enable key.

7.2.2.4 Station Door Controls

This panel provides pushbuttons with visual indicators for releasing the magnetic door locks and opening the door. The buttons are inactive if the proper access conditions have not been established. The position of the stations, the number of doors at each station, and other design requirements determine the number of these panels at each beamline.

7.2.2.4.1 Door/Shutter Interlocks

The door open command is interlocked to the shutter-closed inputs, the Chain-C PLC outputs for the solenoids, and the shutter open from the push button or EPICS for PS2, SS1 and SS2 shutters. To open a door the shutter closed inputs must indicate closed and the status flags must show the door open sequence has not started. The shutter open command is interlocked to the door open push button, the crash button(s), the internal door locked status, and the searched and secure output. The searched and secure output is set true at the successful completion of the search and secure procedure (which includes the closing of all station doors as monitored by the door-closed switches).

The searched and secure signal is set false when a door-closed switch indicates the door is not closed.

A door not closed is detected in approximately 50 milliseconds.

7.2.2.4.2 Pneumatic Door Emergency Egress

The "Emergency Egress" push button is a Life Safety Code Requirement to prevent someone from being locked in a station with pneumatically operated doors.

The "Emergency Egress" push button pneumatically operates the PSS pneumatic door controls to open the station door independent of the PSS. PSS will receive an input indicating when the button has been pressed. This input will be used to sync the door control logic to the position of the door and to prevent a lock failure fault. The PSS locks pneumatic doors 1 second after the closed sensor shows closed and will be re-locked 1 second after a successful search and secure has completed.

7.2.2.4.3 Manual Emergency Door Lock Release

The "Emergency Door Lock Release" push button is a Life Safety Code Requirement to prevent someone from being locked in a station with only manually operated doors.

The "Emergency Door Lock Release" push button is wired in series with the PSS output to the door lock. This push button is located inside of the station near the door it will release. When pressed in it disconnects the lock from PSS. This is true at any beamline station where the station has only manual doors. PSS will monitor this signal to determine if there is a lock failure. Manual doors are locked 1 second after a successful search and secure is completed.

7.2.2.5 System Fault Resets

Each beamline requires two keyed fault reset inputs. The users do not use these keys. The keyed fault reset inputs provides the means to reset PSS faults. Two categories of faults have been determined, and each is reset by its own key. The two keys are for minor and major fault resets.

Major Fault (results in an APS storage ring abort). Typical faults include:

- One of the PLC chains fails
- A PLC major fault

Minor Fault (no abort). Typical faults include:

- Station door close failure
- Safety shutter air manifold pressure low

The PSS System Manager or his designee resets a major fault with a key. A minor fault is reset with a key by the Floor Coordinators.

7.2.2.6 PSS Station Search and Secure

7.2.2.6.1 Overview

The station search and secure process for a beamline station is an Administratively Controlled Procedure (ACP). During the search process, the person performing the search verifies that no one remains inside the station. The PSS system Chain-A PLC enforces an orderly, sequenced and verified walk through of the station along a path providing line of sight to all spaces that could be occupied by a human. The search must end outside the station with all station doors closed. It completes one of the required interlocks needed to open the shutter protecting the station.

The inside of the station contains one or more search buttons with visual and audible indicators of a search in progress. The number of search buttons is determined during the BRC design review process and is based on the design of the enclosure and the equipment it will contain. The search buttons must be depressed in the correct sequence, and the search must be completed and the door closed within a predetermined interval for the search to be considered successful by the PSS logic.

7.2.2.6.2 Implementation

Each search box in the station has an illuminated push button. When the interlocks are satisfied for a search to start, the illuminated push button on search box 1 will start flashing at a one second on, one second off, rate. ***Pressing the push button on search box 1 starts the search sequence***. There is a maximum amount of time allowed to search a station. If the maximum search time is exceeded the search will abort and will have to be started from the beginning. There is no minimum search time.

7.2.2.6.3 Interlocks required to start a search

The interlocks required to start a station search will vary according to the actual station configuration. The items that will vary are the number of emergency stop push buttons, the number of doors and whether the beamline has a mode shutter.

The following interlocks can prevent the search from starting:

- A minor or major fault present.
- The shutter protecting the station is not closed.
- An emergency stop button is pushed in, in the station being searched.
- The station doors are not open or closed as required for a search to begin.
- The user key for the station is turned off.
- The beamline has a mode shutter and a valid mode has not been selected.
- The station is already searched.

7.2.2.6.4 Searching All Stations

When the search sequence is started an audible and a visual warning are also started.

7.2.2.6.5 Audible Warning

The audible warning is a voice announcement of "Searching Station x Exit Immediately". The audible warning is repeated continuously during the search process until the search is successfully completed, the search is aborted or a minor or major fault is detected.

If the search process has successfully completed, the audible warning will continue for an additional 20 seconds to allow anyone missed by the search process and remaining in the station to reach and press an emergency stop button. The emergency stop button will prevent opening the shutters and allowing beam into the station.

If the search process has aborted, the voice announcement of "Searching Station x Exit Immediately" will stop and a voice announcement of "Station x Search Invalid" will be started. The search invalid message will continue for approximately 2 times before the search abort process is considered complete and a new search is allowed to start.

Note that ES&H, DOE 420, NCRP Report 88 and SLAC 327 all require an audible announcement, however only ES&H chapter 5-16 defines a 20 second time requirement.

7.2.2.6.6 Visual Warning

The visual warning consists of one or two red strobe lights that are turned on at the start of the search. The strobe lights will remain on until the search has completed or has been aborted by one or more of the conditions listed under Aborting the Search. See below.

7.2.2.6.7 Searching Stations with Only Manually Operated Doors

After the search box 1 push button has been pressed to start the search the illuminated push button will stop flashing and turn on continuously. Search box 2 will start flashing until pressed. The PSS system will continue flashing each search button in sequence and acknowledging the pressing of the button by turning the flashing indicator on continuously. When the last or only door has been closed, ***the final search box that will be located outside the station must be pressed to complete the search sequence.*** One second after the search sequence is complete the PSS system will lock all doors.

7.2.2.6.8 Searching Stations with Pneumatically Operated Doors

After the search box 1 push button has been pressed to start the search the illuminated push button will stop flashing and turn on continuously. Search box 2 will start flashing until pressed. The PSS system will continue flashing each search button in sequence and acknowledging the pressing of the button by turning the

flashing indicator on continuously. ***When the last or only door has been closed, the search sequence is complete.*** One second after the search sequence is complete the PSS system will lock all doors.

7.2.2.6.9 Aborting the Search

When a search is in progress the search will abort if:

- A search box button is pressed out of sequence.
- A door is closed out of sequence.
- A minor or major fault occurs during the search.
- The search takes to long and times out. Typical maximum search times are 60 to 90 seconds.
- An emergency stop button is pushed in the station being searched.
- The user key for the station is turned off.

In all cases where a search is aborted, the Audible Abort Warning and the Visual Warning will remain enabled for approximately 2 message times from the start of the event causing the search to abort.

The User Key is a convenience key allowing the user to prevent beam into a specific station when off. The User Key enabled is required to start and complete a search and secure procedure. Once the search and secure procedure is complete turning off the User Key will not negate the search and secure status, it will prevent beam from being introduced into the station as a shutter open permit. Further, if the User Key is turned off while the protective shutter is open the shutter will be closed and no fault will be generated.

7.2.3 Shutters and Other Beam Stopping Devices

7.2.3.1 PSS System Controlled Devices - Front End Shutters

FES Shutter Open Operation

When all Front End Shutter permits are true the PSS will allow PS2, SS1 and SS2 to open. The actual opening of the Safety Shutter group is initiated by the user pressing the shutter open button on the user panel or the remote shutter interface (controlled by the user) turning on the proper shutter open signal.

When opening the shutter PSS will always open SS1 and SS2 first. PS2 will not be opened until both SS1 and SS2 have turned on the open limit switches for one (1) second. Then PS2 and possibly PS1 (if PS1 is not already open) will be opened. At

the start of the open process PSS will start a ten (10) second timer. The open process is terminated upon either of three (3) conditions.

Normal open:

SS1 and SS2 shutters open followed by a one (1) second de-bounce delay. This is followed by PS2 and possibly PS1 (if PS1 is not already open) opened followed by a one (1) second de-bounce delay. Thus a normal open will take an average of 2.3 seconds to have the shutter fully open.

The open process will exit and terminate at 3.3 seconds from initiation in this case.

Faulted open:

The FES shutter open process takes several scans of the PLC program to complete. It is possible for the program to detect a fault occurring on any of these program scans. If a minor or major fault is detected the shutter open process will exit and terminate immediately.

Timed out open:

The ten (10) second timer started at the start of the open process timed out and neither a Normal open occurred nor did a Faulted open occur. The status of the four (4) shutters is such that a least one (1) shutter is not on the open limit switch for that shutter. The actual fault identifying the failure is set with common shutter fault detection in the main program process and will result in a No Switch or a Mix-Up fault.

User Aborted open;

The user may abort the shutter opening sequence by either pressing the shutter close button or using the remote shutter close function. PSS will always honor the shutter close commands and override any open command in progress.

FE-EPS Monitoring of open;

FE-EPS monitors PS1, PS2 SS1 and SS2 closed and open switches. If SS1 and SS2 are not both on the open limit switches and both PS1 and PS2 are not on the closed limit switches for three (3) seconds FE-EPS will turn off the storage ring permit dumping the beam.

7.2.3.2 PSS System Controlled Devices - Integral Shutters

Integral shutters are defined as all shutters down stream from the Front End shutters that are not mode shutters. Integral shutters have been designed to stop either monochromatic or pink beam. The monochromatic shutters are air-cooled and contain two beam-stopping devices in series. The beam stopping blocks are usually made of tungsten and either one will stop the beam. The shutters are referred to as

mono stop 1 and mono stop 2 or MS1 and MS2. The shutters MS1 and MS2 are always operated together. If either shutter fails to operate correctly a minor fault will be generated closing all shutters on the beamline. The pink beam shutters are water-cooled and also contain two beam-stopping devices in series. The beam stopping blocks are also made of tungsten and either one will stop the beam. These shutters are also referred to as mono stop 1 and mono stop 2 or MS1 and MS2. The shutters MS1 and MS2 are always operated together. If either shutter fails to operate correctly a minor fault will be generated closing all shutters on the beamline. These shutters require the user BL-EPS system to provide permit allowing them to open. Removal of the user BL-EPS permit when the shutter is open will close the shutter.

7.2.3.3 PSS System Controlled Devices - Mode Shutters

7.2.3.3.1 Mode Control Logic for P4 and P6 Shutters - Overview

The P4 and P6 Mode shutters are two state devices. The P4-20 shutter is used with ID (Insertion Device) Beamlines and the P6-20 is used with BM (Bending Magnet) Beamlines. They may be placed in a Mono Mode or in a Non-Mono Mode (Pink or White Mode). The Mode the shutter is in determines the type of beam that will pass through the device. There are no other valid operational positions of these shutters. These shutters may not assume an intermediate operating position. The beam line must have a valid mode selected to allow operation of any other shutter including the Front End Shutters (FES).

7.2.3.3.2 Mono Mode Operation

In the Mono Mode the shutter will block or stop white beam and acts as a white beam stop. ***APS policy requires the shutter to be mechanically locked while acting as a white beam stop***. Therefore, the PS (Photon Stop) and the SS (Safety Stop) of the shutter are mechanically locked in position by Kirk lock plungers in this Mode. Additionally, the MS1 and MS2 portion of the shutter acts as an integral shutter, passing Mono beam when open and blocking or stopping Mono beam when closed. In Mono Mode the shutter requires the external user signal BL-EPS (Beam Line Equipment Protection System) permit to open MS1 and MS2 and pass Mono beam. If this permit is not present the shutter (MS1 and MS2) will not open. If this permit is removed while the shutter is open, the shutter (MS1 and MS2) will close. Note: the removal of any permit for an open shutter will not generate a fault; it will simply close the shutter. The shutter also requires the PSS system to determine that the down stream critical section is Beam Ready. A beam line critical section is the area from a beam blocking or stopping device (shutter) controlled by PSS, in the direction of beam travel, to the next beam blocking or stopping device. These shutters require the user BL-EPS system to provide permit allowing them to open. Removal of the user BL-EPS permit when the shutter is open will close the shutter.

7.2.3.3.3 Non-Mono Mode (White or Pink Mode) Operation

In Non-Mono Mode (White or Pink Mode) the shutter will block or stop any Mono beam that may be present and will pass the Non-Mono (White or Pink) beam. In this

mode the shutter is effectively removed from the beam path and the control of the beam presence or absence is performed by the next up-stream (in the direction opposite beam travel) shutter. The next up-stream shutter is usually the FES (Front End Shutter). The shutter is open to pass Non-Mono beam. In this mode the next up-stream shutter, usually the FES, requires the user BL-EPS system to provide a permit allowing them to open. Removal of the user BL-EPS permit when the shutter is open will close the shutter.

User Mode Selection Logic for a mode shutter is accomplished as follows:

1. Reset any beam line faults that may be present.
2. Move all 3 keys to the P4 Device Kirk locks and turn them to retract the lock plungers.
3. This will cause a device reset allowing mode selection to take place.
4. Push the Mono or Non-Mono (White/Pink) push button located on the electrical interface enclosure attached to the shutter table to select a mode.
5. The Non-Mono (White/Pink) Mode simulated LED indicator located on the Station Status display will flash when the White/Pink push button is pushed and the shutter assumes the White/Pink position.
6. The Mono Mode simulated LED will flash when the Mono push button is pushed and the shutter assumes the Mono position.
7. Move appropriate keys back to Mode Controller Panel.
8. The selected Mode (Mono or White/Pink) simulated LED will be flashing.
9. Insert the Mode select key into the Mode select key switch on the Mode control panel and turn it to lock in the selected node.
10. The selected Mode (Mono or White/Pink) simulated LED will now remain continuously on to indicate the shutter mode.
11. Remove the Mode select key from the panel.
12. This completes mode selection.

User panel Mode Indicator Operation

- MONO MODE INDICATOR

Green Indicator This Indicator will be blink when the user has positioned the Kirk lock keys in the correct locks for Mono mode. This Indicator will be on (not

blinking) when Floor coordinator locks in the Mono mode by toggling the Mode Select key in the mode select lock. This Indicator will be off for all other conditions. Chain C using internal logic to indicate to the user that a valid mode is selected and locked in position for the mode shutter controls this Indicator.

- NON-MONO (PINK/WHITE) MODE INDICATOR

Green Indicator This Indicator will be blink when the user has positioned the Kirk lock keys in the correct locks for Pink/White mode. This Indicator will be on (not blinking) when Floor coordinator locks in the Pink/White mode by toggling the Mode Select key in the mode select lock. This Indicator will be off for all other conditions. Chain C using internal logic to indicate to the user that a valid mode is selected and locked in position for the mode shutter controls this Indicator.

- NONE MODE INDICATOR

Red Indicator This Indicator will be on when the Kirk lock keys are NOT in the correct locks and captured (turned to the non-removable position) for Mono mode or Non-Mono Mode (Pink or White Mode). This Indicator will be off if either of the Mono mode or Pink/White mode Indicators are blinking or on. Chain C using internal logic to indicate to the user that a valid mode is NOT selected and/or locked in position for the mode shutter controls this Indicator.

The following table defines the mode information to the user through the BL-EPS interface.

Description	Mode 2	Mode 1
All keys are detected in shutter. Allow Mode Change.	X	1
A Valid Mode Reset has occurred. The Beamline is in Mono Mode.	0	0
A Valid Mode Reset has occurred. The Beamline is in Non-Mono Mode (Pink or White Mode).	1	0

7.2.3.4 Manually Controlled - PSS System Monitored

7.2.3.4.1 Manual Beam Stops

There are two special cases of beam blocking or stopping devices in addition to a shutter controlled by PSS.

Manual Beam Stops (MBS) are manually operated beam stopping devices that do not allow any beam down stream of their location. When closed a MBS very effectively ends the beamline and any stations down stream of the MBS location will no longer be monitored by the PSS for programmed faults. The MSB itself of course must be

monitored to insure it remains closed. The PSS monitors the Closed Input Status switches. There is no BL-EPS Permit for the MBS, but there is a BL-EPS Closed Status output available to the user via the BL-EPS interface. Stations down stream of a closed MBS retain the PSS functions to open and close station doors only.

The other beam blocking device is the fixed beam stop located at the end of the last station in the beam line. This beam stop will absorb the full power of any beam reaching the end of the beamline.

7.2.4 PSS System Interfaces

7.2.4.1 Access Control Interlock System (ACIS) interface with PSS

All beamlines have a Global on-line/off-line key switch located in a junction box associated with each storage-ring sector and located atop the storage ring shielding enclosure. The junction box is the interface point for the two PSS systems associated with each sector and the ACIS system. Because the enclosure contains circuitry maintained by the ACIS staff, access is limited to the ACIS and APS control room operators.

Inside the junction box are located the on-line/off-line key switches, one for each of the two beamlines associated with the sector. When the key switch for a beamline is set to off-line, its safety shutters and the second photon shutter are prevented from opening and the PSS beam-dump signal is ignored. When the key switch is set to on-line, the shutters will be allowed to open under PSS control and the ACIS monitors and reacts to the beam-dump signal from the PSS. The key switches are under the control of the APS control room staff, and their use is strictly governed by administrative procedures. The key switch is set off-line until the beamline has been authorized to begin commissioning/operation. The key switch is also set off-line when the PSS is undergoing maintenance or testing during storage-ring operation.

The Global On-Line permit also controls a solenoid supplying control air to the solenoids for PS2, SS1 and SS2. When the permit is true (on) the solenoid is energized allowing air to the PS2, SS1 and SS2 solenoids. When the permit is false (off) the same solenoid vents the supply to the PS2, SS1 and SS2 solenoids to atmosphere closing the shutters if they are not already closed.

There is also a permit identified as the ACIS Front End Shutter permit. This permit originates at an administratively controlled key switch located in the accelerator control room. It is distributed to all beamlines and will cause the PSS at each beamline to close any open Front End Shutters when the permit is removed (turned off). When the ACIS Front End Shutter permit is enabled (turned on) the Front End Shutters may be opened at the beamlines. Opening the Front End Shutters is not automatic, they must be opened by an operator pressing the shutter open button or turning on the appropriate input to the Remote Shutter Interface (RSI).

7.2.4.2 Front End Beamline Shutters

The Front End Shutters are actually 4 individual shutters operated together as a group. There are two photon absorber shutters PS1 and PS2. These shutters are water cooled and designed to withstand continuous direct beam from the storage ring. The PS1 shutter is located nearest the storage ring and used as a backup to be closed if the PS2 shutter cannot be closed for some reason. Therefore the PS1 shutter is normally kept open. If it is not open, it will be opened simultaneously with PS2. The other two shutters are Bremsstrahlung safety stops and are named SS1 and SS2. These shutters are not designed to stop direct beam and must be protected by PS1 or PS2. The SS1 and SS2 shutters are operated together. The PSS Emergency Shut Down (ESD) systems are redundantly wired to the shutter open limit switches of all 4 shutters. The PSS ESD systems receive redundant shutter closed status for all 4 shutters from the ACIS interface. Chain-C operates these shutters by turning on the appropriate outputs that are routed through relays controlled by Chain-A and Chain-B to solenoids that operate the pneumatic cylinders attached to each shutter.

These shutters are always sequenced open by opening SS1 and SS2 first. When SS1 and SS2 are confirmed open PS2 is opened. If PS1 is closed it is opened with PS2.

These shutters are always sequenced closed by closing PS2 first. If PS2 fails to close, PS1 is commanded to close by turning off its output. If PS1 fails to close and PS2 failed to close the storage ring is dumped. If PS2 failed to close, but PS1 closed successfully, the storage ring is not dumped. However, a fault will be generated identifying the PS2 failure and preventing beamline operation until the problem is identified, corrected and the fault successfully reset. When PS2 or PS1 are confirmed closed SS1 and SS2 are closed.

Control of these shutters depends on several interlock signals.

When ACIS Global On-Line is true the Front End Shutters may operate. When false the Front End Shutters may not operate and the energy source is removed.

When the ACIS Front End Shutter permit is true the shutters may be opened. When the ACIS Front End Shutter permit is false any open shutters are closed and may not be reopened.

When the FE_EPS Front End Shutter permit is true the shutters may be opened. When the FE_EPS Front End Shutter permit is false any open shutters are closed and may not be reopened.

7.2.4.3 Front End Equipment Protection System (FE-EPS) interface with PSS

There is an interface between the PSS and the FE-EPS systems that allows the FE-EPS system to control operation of the Front End Shutters to a limited degree. The FE-EPS supplies PSS with 2 signals; the FE_EPS Front End Shutter permit and the FE-EPS PS1 open request.

The FE_EPS Front End Shutter permit signal is a permit to PSS. When true the PSS may open the shutters PS2, SS1 and SS2 at the request of the user if all interlocks are present. If the Front End Shutters are open FE-EPS can cause the PSS to close the shutters by setting the permit to false or off. Removal of a permit will not cause a fault!

The FE-EPS PS1 open request signal is a request to the PSS to open the PS1 shutter and is independent of operation of PS2, SS1 and SS2. The PSS will open PS1 if PS2, SS1 and SS2 are closed. If PS2, SS1 and SS2 are already open, (allowed by the FE_EPS Front End Shutter permit being true) PS1 was opened with PS2. If the user presses the close button for the Front End Shutters and the FE-EPS PS1 open request is false, when PS2, SS1 and SS2 are fully closed PS1 will be closed also.

The PSS supplies the FE-EPS system with 4 signals. The signals are the status of the open shutter limit switches for PS1, PS2, SS1 and SS2.

7.2.4.4 Beamline Equipment Protection System (BL-EPS) interface with PSS

The beamline user must provide the beamline equipment protection system. The purpose of the interface is to allow the user to define their own protection criteria for their equipment and cause the PSS to close a protective shutter if the equipment is in danger. There must be a permit supplied by the user for each shutter down stream of the Front End Shutters. When true (on) this permit will allow the PSS to operate the shutter. When false (off) the PSS will close the shutter if it is open and will not allow it to be reopened.

The interface also provides to the user the status of a mode shutter if there is one installed. For each shutter or manual beam stop down stream of the Front End Shutters the inter face provides the user with shutter closed status.

7.2.4.5 De-Ionized water (DIW) interface with PSS

The de-ionized water system is used to cool beam stopping or beam shaping devices that receive a high heat load and must be cooled to prevent component damage. The PSS monitors de-ionized water flow and pressure with a self contained PSS chassis containing set point controllers for each required flow loop. The set point controllers are programmed to be fail-safe and will trip on loss of power or operation beyond a programmed set point. There is an independent controller for Chain-A and one for Chain-B. Chain-A will normally monitor flow through the critical component. Chain-B will normally monitor differential pressure across the critical component. The Safety Interlocks Group is responsible for the controller chassis and the cabling to the transducer cabinet. Another group is responsible for the de-ionized water system, including the transducers and the cabinet that houses them.

7.2.4.6 HMI interface with PSS

The Human Machine Interface (HMI) is a touch screen terminal that will display the PSS status for each station and for the entire beamline. It will also display PSS

diagnostic information and provide touch sensitive areas for the user to control door and shutter operation. The Human Machine Interface (HMI) interfaces with the PSS through Chain-C using an Ethernet connection.

7.2.4.7 EPICS interface with PSS

There is an EPICS interface that connects the beamline PSS to the APS control system. This allows EPICS and related systems to display and archive system operation as well as provide limited control of the beam line through Chain C. The only functionality provided at this time is the ability to remotely open and close the beamline shutters through EPICS. Chain C will reject illegal or unsafe commands from EPICS and issues the command to open the front-end shutters only if all interlocks allow it. Remember the shutter close command is always operational locally, and remotely if desired, and will always override a shutter open operation. Regardless of the state of Chain C, the safety interlock PLCs will not allow the shutters to open if the PSS is not secure and will trip the ACIS if an unsafe safe condition is detected while the shutters are open.

7.2.5 PSS Control System

7.2.5.1 Command and Control

The command and control functions are provided by a separate PLC called Chain-C. The Chain-C PLC provides all beamline user operational capability including PSS status and PSS control. Also provided by Chain-C is a safe PSS interface to the outside world for status and limited control.

First, Chain-C keeps track of the status of the entire PSS for the beamline. The information is received by Chain-C from its own sensors, from Chain-A and from Chain-B. Chain-A and Chain-B transmit the status of all critical inputs and outputs and any detected faults continuously to Chain-C. This transmission of information is in the form of a broadcast and provides no mechanism for Chain-C to write to Chain-A or Chain-B. Chain-C has an interface to local beamline display(s) to provide the user with PSS Status. Chain-C also has an interface to EPICS providing status to the much larger audience connected to the control network.

Second, Chain-C interfaces to the user accessible controls for operation of the beamline shutters, doors, several enabling key switches, mode shutter operation and other devices that may be required by a particular beamline configuration.

Third, Chain-C interfaces to EPICS to provide the user the ability to remotely and possibly programmatically control shutter operation for the beamline. This interface for shutter control is not different from the local control provided by Chain-C and is subject to all of the interlock conditions of the local control.

And finally, Chain-C causes the desired user actions, such as opening a shutter or closing a door, to happen by turning on or off its outputs. For all critical devices such

as shutters the output from Chain-C is routed through the normally open relay contacts of Chain-A and Chain-B before reaching the controlled device.

7.2.5.2 Emergency Shutdown

The Emergency Shut Down (ESD) or protective interlock component of the PSS is provided by two PLCs connected in a series configuration. The PLCs used are manufactured by different major vendors to reduce common mode failure factors. They are further programmed by different individuals to decrease the probability of common mode implementation issues. The two PLC systems are named Chain-A and Chain-B.

The two ESD systems will monitor the status of the each station and the protective shutter for each station.

All critical sensors are redundantly provided and wired directly to each ESD Chain. The sensors for the door-closed status are of different manufacturers and technologies. Chain-A has an electronic sensor and Chain-B has a mechanical sensor. The shutter position limit switches are of the same manufacture but are redundant and independently wired to each ESD Chain. The Emergency Beam Stop button is an industrial e-stop switch wired independently to each ESD Chain.

Search and secured is an administrative procedure enforced and monitored by Chain-A. The resulting search status is provided as an interlock to Chain-B and Chain-C by Chain-A.

If the station has been searched and secured a successful search has taken place and the station doors have been closed and locked. The Emergency Beam Stop buttons in the station are not pressed in. The station will assume the *BEAM READY* state. At any time while in the *BEAM READY* State the protective shutter for the station may be opened. If the shutter protects more than one station all stations protected must be *BEAM READY* for the shutter to be allowed open. When the shutter is opened the station will also be in the *BEAM ACTIVE* state. Note that a shutter is considered open if any component of the shutter cannot positively be determined to be closed.

If any of the safety interlocks necessary for the station to remain *BEAM READY* are removed while the station is *BEAM ACTIVE* the PSS will remove the storage ring permit to the ACIS and the ACIS will dump the storage ring.

Any trip of either ESD system will require a key switch reset to continue operation.

The PSS system uses the following fault detection and reporting mechanism to prevent unsafe operation of the beamline.

7.2.5.2.1 PSS Fault Operation and Tag Name Descriptions

PSS faults are dependant upon the beamline Station status. Each Station will be in one of the following status states. Cumulatively the states of all Stations represent the status of the beamline.

PSS Station Status States:

OPEN ACCESS

The Station has not been successfully searched. The Station door(s) may or may not be open. Additionally, the user has no restriction against opening any door.

SEARCHED & SECURE

The user has successfully searched the station and the station doors have been locked. A *SEARCHED & SECURE* Station is not necessarily *BEAM READY* as SEARCHED & SECURE is only one of the interlocks required for *BEAM READY*. The user has no restriction against opening any door. However, if the user opens a door the station status will revert to *OPEN ACCESS*.

BEAM READY

All of the interlocks for the Station are in a state to allow operation of the shutter protecting the Station. The interlocks necessary for *BEAM READY* are:

The station must be *SEARCHED & SECURE*.

All of the station doors must show closed.

The User Key must be turned and captured by the lock.

The station must be APS Enabled. A floor coordinator inserting the APS Enable key and toggling the interlock to true performs this.

The ACIS Global On-Line Key permit must be enabled for both Chain-A and Chain-B ESD systems.

The ACIS Front End Shutter permit must be enabled in the control room.

The Station crash button(s) must not be pressed in.

There may not be any detected fault conditions.

BEAM READY and BEAM ACTIVE

The shutter or shutters between the Station and the Storage Ring are NOT closed thus allowing bean into the Station. The station must remain *BEAM READY* to remain *BEAM ACTIVE*. During normal operation the station status will change from *BEAM READY* to *BEAM READY and BEAM ACTIVE* when the user opens the protective

shutter. The status will revert to *BEAM READY* when the shutter is closed. There are additional interlocks necessary to open the shutter and they are:

All station doors must indicate they are locked internal to PSS.

If there is a mode shutter a valid operating mode must have been selected for it.

RESTRICTED ACCESS

PSS has determined the station is beam active because the shutter(s) protecting the station is or are not closed. The user is prohibited from accessing the Station by PSS. PSS will keep the Station doors locked until the shutter has been successfully closed. It may be necessary to remove the air to the Front End Shutters to close them and remove all beam from the beamline. After appropriate personnel verify there is no beam in the Station the locked door(s) may be opened by use of the door pneumatic panel if it should be necessary to gain access to the Station prior to closing the shutter.

PSS Fault Types and Characteristics:

Major faults will dump the Storage Ring (drop the SR permit). On (Touch Screen) systems the Major Fault indicator will flash at a .5 second on, .5 second off rate.

Minor faults will not dump the Storage Ring. The Minor Fault indicator will be flashing at a .5 second on, .5 second off rate.

Warning faults will not dump the Storage Ring. The Warning Fault indicator will be flashing at a .5 second on, .5 second off rate. At this time the only warning fault in use is Door Lock Failure. A failed door lock does not prevent beamline operation. It is displayed as a maintenance information item indicating the need to repair a defective lock. The lock is used to prevent a challenge to the PSS system closed doors and thus a possible Storage Ring dump, but is not required for safe operation of the beamline.

Common fault Characteristics

There will be individual simulated indicators for each fault type so there will be no confusion as to fault type. All faults, except *Warning* faults, close all open shutters. Shutters that have a photon absorber and two safety stops and the Front End Shutters will ***always*** be sequenced open and closed. All faults are latched by the system and require a manual reset with a key for beamline operation to resume.

While all detected faults except *Warning* remove front-end shutter permits, only a *Major* fault generates a PSS trip to the ACIS.

Examples of the more common faults are in the following table. However, you must refer to the PSS Beamline Fault document for the faults that apply to that beamline and version of operational software.

FAULT TAG	FAULT TYPE	MEANING
PSS_CHAIN_A_DEAD	Minor	Chain-A has stopped running or the watchdog relay has failed. If Chain-A stopped running the storage ring is dumped due to removal of the permit to ACIS.
PSS_CHAIN_B_DEAD	Minor	Chain-B has stopped running or the watchdog relay has failed. If Chain-B stopped running the storage ring is dumped due to removal of the permit to ACIS.
CHAINA_POWER_UP	Major	Chain-A has been power-cycled and will not start running until the Major fault reset key switch is toggled to clear this fault.
CHAINB_POWER_UP	Major	Chain-B has been power-cycled and will not start running until the Major fault reset key switch is toggled to clear this fault.
x_CBn_PUSH_BEAM_ACTIVE	Major	A crash button (n) in station (x) was pushed, while the station was in the BEAM ACTIVE state.
x_DRn_OPEN_BEAM_ACTIVE	Major	The station (x) door (n) closed switch input indicates NOT Closed while the station is in the BEAM ACTIVE state.
x_NO_SS_BEAM_ACTIVE	Major	The station (x) indicates it is no longer searched and secured while the station is in the BEAM ACTIVE state.
x_MBS_MOVED_BEAM_ACTIVE	Major	The station (x) Manual Beam Stop (MBS) moved off then closed switches while in the BEAM ACTIVE state.
x_SHTR_yyy_BOTH_SWITCH	Minor	The shutter protecting Station (x) is in an ambiguous detected position (both open and closed limit switch inputs are true). ***This should never happen. The station will be treated as beam active until proven safe by other means.***
GLBONLN_OFF_BEAM_ACTIVE	Minor	The Global On-Line permit from the ACIS was removed with the Front End Shutters NOT closed.
FE_PRESS_GT_60_FAILED	Minor	If the Global On-line permit is present the greater than 60 psi switch should be true. If the Global On-line permit is absent the

FAULT TAG	FAULT TYPE	MEANING
		greater than 60 psi switch should be false. This signal is checked in both directions to detect faulty or un-calibrated switches.
FE_PRESS_LT_3_FAILED	Minor	If the Global On-line permit is absent the less than 3 psi switch should be true. If the Global On-line permit is present the less than 3 psi switch should be false. This signal is checked in both directions to detect faulty or un-calibrated switches.
PLC_KEY_TO_REM	Minor	A PLC has been switched from "RUN" to "REMOTE".
x_SHTR_PRESS_LT_60_PSI	Minor	There is insufficient air pressure for shutter control in the x station. Sufficient air pressure is >60 psi.
MODE_RES-ACTIVE	Minor	Someone has toggled a key in the Beam Mode PSS panel while the beamline is in the BEAM-ACTIVE state.
x_DR_CLSE_FAIL	Minor	The x door has failed to remain closed (as indicated by the door closed switch) after it has been successfully closed and locked.
x_CBn_PUSH_STATION_SECURE	Minor	The crash button (n) in station (x) has been pushed after the station has been searched and secured.
x_FLOW_LOSS	Minor	Cooling water flow has been reduced to below whatever the particular set point for that particular instrument was.
x_REMOTE_IO_COMn_FAILURE	Minor	Shows that one of the remote I/O modules is not communicating or has faulted, and identifies exactly which one. The x identifies which station, and the n identifies which module is faulted. This fault may also cause a major fault if the station is beam active and the doors show open.

7.3 PSS Testing and Configuration Control

7.3.1 PSS Testing Overview

The PSS implementation provides a means to operate the system in a test mode with the critical front-end safety and photon shutters disabled in the closed position. This is referred to as the

Global Off-Line State and allows storage ring operations to continue while the beamline is being tested.

System testing provides the single most important contribution to safe operation. Since few failures arise during operation, a rigorous testing program has been developed that includes all the protective elements of the system. There are written procedures to verify the systems integrity following any maintenance, addition of new components, or software changes.

The validation process verifies that the PSS operates as designed and that abnormal or out-of-sequence events do not result in an unsafe condition. Testing of the system is performed before the system is placed in service, after any maintenance, and at periodic intervals of at least once a year in compliance with DOE Order 5480.25 and DOE Order 420.2. The PSS validation procedures are under document control.

The type of testing used to validate the PSS is stimulus response testing. Normal behavior of the PSS is defined and white box testing is used to validate the proper system response. Abnormal operator or component behaviors are also tested by determining what is possible, including simultaneous events, and testing for a proper PSS system response.

7.3.2 Manual Validation Test System

The manual validation system consists of several carts using a master / slave configuration containing remote I/O that is connected to the PSS by plug in cables. A cover is used to secure the test connections to the PSS. Two limit switches monitor the position of the cover. The cover prevents inadvertent tampering with the test inputs. Additionally, when the test connector cover is opened, the beamline Front End Shutters are disconnected from the PSS using the limit switches and relays. Also, The limit switches and relays will remove both Chain-A and Chain-B storage ring permits to the ACIS. The test system only connects to the inputs and outputs of the two Emergency Shut Down (ESD) systems. The test cart receives 24 VDC power from the PSS and connects to the communication buss cable for communication to the master cart. The master test cart (usually located at beamline Station A) controls all of the testing of the ESD systems by removing ESD sensor power, controlling the ESD input signals by injection, and monitoring the ESD output. This provides a means to test and verify the functionality of both ESD systems independently for proper response to normal and off normal conditions and may be automated in the future. It should be noted that the initial testing will start with an I/O check to verify all wiring and signal paths to the sensors and controlled devices are in tact and the devices are functioning correctly. In addition, a communication failure test is performed to verify all outputs respond properly by turning off when communications is lost. The master test cart may be plugged in and used at any location equipped for a test cart. There are certain conditions that remain to be tested by other means, as they are a part of the test system. An example would be validation of test connector cover safety switches. These switches will operate as a part of the process of plugging in the test cart and therefore can't be tested by the cart. It should be noted, when the test cart system is removed from the beamline a final end-to-end test must be performed on all critical devices.

7.3.2.1 Test Connections and Trip Criteria

The Front End Shutters must be closed and the beamline Global On-Line permit removed (off). When the tester is connected to a PSS, the connections between the PSS output modules from Chain-A and Chain-B that provide the storage ring permit to the ACIS are opened thus generating a constant PSS Storage Ring trip to the ACIS.

This guarantees the ACIS will trip the storage ring and dump stored beam when:

If the beamline Global On-Line permits is restored before securing all of the test system connector covers. Remember the storage ring permits have been removed by opening the test system connector covers.

If the beamline Global On-Line permit is false (off) and any Front End Shutter is NOT CLOSED (PS2, SS1 or SS2). Note PS1 is not included in this logic.

7.3.2.2 Mezzanine Test Components

There will be a mezzanine test cart containing the I/O for the test system. This cart is unique to testing the PSS components located on the mezzanine and is not interchangeable with a test cart used on the experimental floor. This test cart like all others, will plug into the test connectors and the test buss communication connector. The test cart is self-contained receiving power through the test connectors. The master test cart will control this remote test cart to stimulate the PSS system and convey the PSS system response to the staff performing the validations.

7.3.2.3 Experimental Floor Test Components

There will be two different test cart configurations used on the experimental floor.

There will be a master test cart containing a touch screen user interface for controlling and monitoring the test progress. It will also contain a PLC to monitor and control the test I/O. This test cart will contain the same test I/O as all floor test carts since the ESD remote I/O on the floor uses a common circuit board. The test connections will be the same at each station containing ESD I/O requiring validation. The touch screen and the PLC will require 120 VAC power. The test I/O will be self-contained receiving its 24 VDC operating voltage through the test connectors. This cart will control the test buss and all test I/O connected to it. The master test cart will control the remote test carts to stimulate the PSS system and convey the PSS system response to the staff performing the validations.

There will be one or more slave test carts containing the I/O for the test system. This cart type is unique to testing the PSS components located on the experimental floor and is not interchangeable with a test cart used on the mezzanine. This test cart like all others, will plug into the test connectors and the test buss communication connector. The test cart is self-contained receiving power through the test connectors.

7.3.3 Lab Beamline Simulator Test System

There will be a system built in the Safety Interlocks test lab that will emulate the hardware behavior of a beamline. The system will contain the same processors and I/O used in the PSS on the experimental floor. This will allow the exact same code that will be loaded on the floor to be loaded and tested in the lab. The system will be used to test and debug all changes to the software used in Chain-A, Chain-B and Chain-C. It will also be used to regression test the software insuring any changes did not break the parts that were not supposed to be changed.

The Lab simulator may seem redundant since the PSS system on the floor must be validated after new or changed software is loaded. The simulator for Version 1 systems has proven to be invaluable for catching mistakes before the Validation on the floor. As an additional benefit the simulator can be used for testing what if scenarios.

Any change to the software due to an error detected during the on floor validation requires the validation start over. This is necessary to insure the correction did not break the functionality already tested. The time saving can be significant if starting over late in the validation is avoided.

2.1 PSS the Future

7.3.4 Automated validations.

The design for the PSS Generation-3 contains the infrastructure to automate the testing and recording of the functional validation of the Chain-A and Chain-B ESD systems. There would many benefits realized from automated testing. Some of the benefits include faster testing, the capability to monitor all connections to the ESD systems as each test is performed insuring detection of undefined behavior, repeatability of testing, the ability to test for race conditions, the ability to accurately time the system response and accurate recording of test results. Of course the test system would have to be validated periodically to insure the testing and recording operate as expected.

7.3.5 Retrofit Capabilities

The design criteria for Generation-3 PSS included consideration for implementation of Generation-3 capabilities at existing beamlines using Version 1 and Version 2 PSS. The design of the Generation-3 PSS contains a super-set of Version 1 and Version 2 PSS systems thus allowing the use of the Generation-3 system to replace the older systems. There remain significant cost issues concerning replacement of the existing old PLC hardware with current components.

Appendix A

ACRONYMS

The following are some of the frequently appearing or unique acronyms used in this document. This list is provided as a quick reference for the reader's convenience.

ACIS .....Access Control and Interlock System
APS .....Advanced Photon Source
ARR.....Accelerator Readiness Review
ASD.....Accelerator Systems Division
BL-EPS .....Beamline Emergency Protection System
CAT.....Collaborative Access Team
DIW.....De-ionized Water
EPICS.....Experimental Physics and Instrumentation Control System
EPS.....Equipment Protection System
ES .....Electrical Systems Group
FDR.....Final Design Review
FE-EPS.....Front End Emergency Protection System
FERDP .....Front End Relay and Distribution Panel
FOE.....First Optics Enclosure
HMI.....Human Machine Interface
ICD.....Interface Control Document
ISIG.....Interlocks Systems and Instrumentation Group
OI .....Operator Interface
PDR.....Preliminary Design Review
PLC .....Programmable Logic Controller
PSS.....Personnel Safety Systems
SRI .....Synchrotron Radiation Instrumentation
TBD.....To Be Decided
XFD.....Experimental Facilities Division

Term Definitions

The following are some of the frequently appearing or unique terms used in this document.

- Term Definition - Down Stream Beam Direction

The direction defined by the path from the Storage Ring to the end of the last Station of a beam line. The beam flow is from the Storage Ring through the Front End Shutters into and through Station A and then to Station B and so on until the beam encounters either a closed Shutter or a beam stop at the end of the last Station.

- Term Definition - Up Stream Beam Direction

The direction defined by the path from the end of last Station of a beam line to the Storage Ring. The direction opposite the flow of the beam.

- Term Definition - Critical Section

The critical section of a beam line is the area from the point of reference or interest, in the up stream beam direction, to the nearest Shutter that can be closed. Reminder, a mode shutter in white beam mode can not be closed, therefore the critical section continues in the upstream direction to the next shutter that can be closed. Notice, the Critical Section will always include one Station, but it may include more than one Station.

- Term Definition - Critical Device

A critical device in a beam line is a device designed to block some or all of the beam and absorb significant power from the beam in the process or to prevent access to the beam.

Examples: Doors, Shutters, Fixed Masks and Beam Stops both movable and fixed.

A critical device is also any device used in the design to monitor the position of any critical device or to prevent or minimize exposure to the beam by causing the closing of shutters or dumping the storage ring.

Examples: Shutter position switches, Door Closed switches and Emergency Beam Stop buttons (Crash Buttons).

- Term Definition - acceptance criteria

Specified bounds on the value of a *functional* or *condition indicator* used to assess the ability of a *structure, system or component* to perform its *design* function.

- Term Definition - failure

Inability of a *structure, system or component* to function within *acceptance criteria*.

! Note that the *structure, system, or component* is considered to fail when it becomes incapable of functioning, whether or not it is needed at that time. A *failure* in, for example, a backup system may not be manifest until the system is called upon to function, either during testing or on failure of the system it is backing up.

- Term Definition - ***common cause failure***

Failure of two or more *structures, systems or components* due to a single specific event or cause.

For example, a *design* deficiency, a manufacturing deficiency, *operation* and *maintenance* http://www.iaea.or.at/ns/CoordiNet/safetypubs/iaeaglossary/glossarypages/m.htm - maintenanceerrors, a natural phenomenon, a man-induced event, saturation of signals, or an unintended cascading effect from any other *operation* or failure within the plant or a change in ambient conditions.

- Term Definition - ***common mode failure***

Failure of two or more *structures, systems or components* in the same manner or mode due to a single event or cause.

i.e. A common mode failure is a type of common cause failure in which the structures, systems, or components fail in the same way.

- Term Definition - failure mode

The manner or state in which a structure, system or component fails.

- Term Definition - ***structures, systems and components (SSCs)***

A general term encompassing all of the elements (items) of a facility or activity which contribute to protection and safety, except human factors.

Structures are the passive elements: buildings, vessels, shielding, etc. A ***system*** comprises several ***components***, assembled in such a way as to perform a specific (active) function.

This is the last page of this document.